IN THE U.S. PATENT AND TRADEMARK OFFICE

Appellants:	Chen et al.
Application No.:	10/621,324
Art Unit:	2416
Filed:	July 18, 2003
Examiner:	Ian N. Moore
For:	METHODS AND DEVICES FOR RE-ROUTING MPLS TRAFFIC
Attorney Docket No.:	129250-000979/US

APPELLANTS' BRIEF ON APPEAL

MAIL STOP APPEAL BRIEF - PATENTS
Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

August 19, 2009

TABLE OF CONTENTS

APPELLANTS' BRIEF ON APPEAL

I. REAL PARTY IN INTEREST:

The real party in interest in this appeal is Lucent Technologies Inc. Assignment of the application was submitted to the U.S. Patent and Trademark Office and recorded at Reel 014306, Frame 0108.

II. RELATED APPEALS AND INTERFERENCES:

There are no known appeals or interferences that will affect, be directly affected by, or have a bearing on the Board's decision in this Appeal.

III. STATUS OF CLAIMS:

Claims 1, 3-5, 7-9, 11-13, 15-17, 19-21 and 23-29 are pending in the application. Claims 2, 6, 10, 14, 18 and 22 have been cancelled. Claims 1, 5, 9, 13, 17, 21, 25 and 28 are written in independent form.

Claims 1, 3-5, 7-9, 11-13, 15-17, 19-21 and 23-29 were rejected under 35 U.S.C.§103(a) based on the combination of U.S. Patent Publication Application No. 20030147346 to Kanakubo (Kanakubo) and U.S. Patent Publication Application No. 20040004937 to Skalecki (Skalecki). Claims 1, 3-5, 7-9, 11-13, 15-17, 19-21 and 23-29 were rejected under 35 U.S.C.§103(a) based on the combination of U.S. Patent No. 7,167,443 to Dantu (Dantu) and Skalecki. Further, claims 1, 3-5, 7-9, 11-13, 15-17, 19-21 and 23-29 were rejected under 35 U.S.C.§103(a) based on a combination of Dantu and U.S. Patent No. 5,838,924 to Anderson ("Anderson").

Claims 1, 3-5, 7-9, 11-13, 15-17, 19-21 and 23-29 are being appealed.

IV. STATUS OF AMENDMENTS:

An Amendment After Final (AAF) was filed on May 18, 2009. In an Advisory Action dated May 29, 2009, the Examiner stated that the AAF was entered but did not place the application in condition for allowance.

V. SUMMARY OF CLAIMED SUBJECT MATTER:

(i). Overview of the Subject Matter of the Independent Claims

The present invention is directed at methods and devices for detecting failures along an "ingress region" of a primary path within an MPLS-based network, and, thereafter, associating an original IP address of a primary path to an alternate path upon detection of the failure. More specifically, independent claim 1 reads as follows (specification citations are in parenthesis):

1. A network device, wherein the device:
detects a failure along an ingress region of a primary path(paragraph [0020])**;**
re-routes traffic from the primary path associated with an original Internet Protocol (IP) address to an alternate path which includes the device using a forwarding table that includes IP and Multi-Protocol Label Switched (MPLS) routing information (paragraph [0020])**while associating the original IP address to the alternate path upon detection of the failure** (paragraph [0020])**; and**
allows traffic to travel along the primary path when the failure is no longer detected along the ingress region (paragraph [0020])**.**

Independent claim 5 reads as follows:

5. A network device, wherein the device:
receives a failure message;
re-routes traffic from a primary path associated with an original IP address to an alternate path using a forwarding table that includes IP and MPLS routing information (paragraph [0020])**, said rerouting maintaining the original address, the alternate path comprising devices which maintain a same quality of service as the primary path**

(paragraph [0032])**and are not a part of the primary path except for the network device and a destination network device** (paragraphs [0021] and [[031])**; and**

allows traffic to travel along the primary path when the failure is no longer detected (paragraph [0020])**.**

Independent claim 9 reads as follows:

9. A method for re-routing traffic comprising the steps of:

detecting a failure along an ingress region of a primary path (paragraph [0020])**;**

re-routing traffic from the primary path associated with an original IP address to an alternate path which includes a source device using a forwarding table that includes IP and MPLS routing information while associating the original address to the alternate path upon detection of the failure (paragraph [0020])**; and**

allowing traffic to travel along the primary path when the failure is no longer detected along the ingress region (paragraph [0020])**.**

Independent claim 13 reads as follows:

13. A method for re-routing traffic comprising the steps of:

receiving a failure message (paragraph [0020])**;**

after said receiving step, re-routing traffic from a primary path associated with an original IP address to an alternate path using a forwarding table that include IP and MPLS routing information (paragraph [0020])**, said rerouting maintaining the original address, the alternate path comprising devices which maintain a same quality of service as the primary path** (paragraph [0033])**and are not a part of the primary path except for an initiating network device and a destination network device** (paragraphs [0021]) and [0031])**; and**

allowing traffic to travel along the primary path when the failure is no longer detected (paragraph [0020])**.**

Independent claim 17 reads as follows:

17. A network device comprising:
means for detecting a failure along an ingress region of a primary path (paragraph [0020])**;**
means for re-routing traffic from the primary path associated with an original IP address to an alternate path which includes the device using a forwarding table that includes Internet Protocol (IP) and Multi-Protocol Label Switched (MPLS) routing information (paragraph [0020])**while associating the original IP address to the alternate path upon detection of the failure** (paragraph [0020])**; and**
means for allowing traffic to travel along the primary path when the failure is no longer detected along the ingress region (paragraph [0020])**.**

Independent claim 21 reads as follows:

21. A network device comprising:
means for receiving a failure message(paragraph [0020])**;**
means for re-routing traffic from a primary path associated with an original IP address to an alternate path using a forwarding table that includes IP and MPLS routing information(paragraph [0020])**, said means for re-routing maintaining the original address, the alternate path comprising devices which maintain a same quality of service as the primary path** (paragraph [0032])**and are not a part of the primary path except for the network device and a destination network device**(paragraphs [0021] and [0031])**; and**
means for allowing traffic to travel along the primary path when the failure is no longer detected (paragraph [0020])**.**

Independent claim 25 reads as follows:

25. A source network device, wherein the device:
detects a failure along an ingress region of a primary path (paragraph [0020])**, where the ingress region comprises a link associated with the source network device** (Figure 1; paragraphs [0004], [0016] through [0018])**;**

re-routes traffic from the primary path associated with an original Internet Protocol (IP) address to an alternate path which includes the device using a forwarding table that includes IP and Multi-Protocol Label Switched (MPLS) routing information (paragraph [0020])**while associating the original IP address to the alternate path upon detection of the failure** (paragraph [0020])**; and**

allows traffic to travel along the primary path when the failure is no longer detected along the ingress region (paragraph [0020])**.**

Independent claim 28 reads as follows:

28. A source network device, wherein the device:

detects a failure along an ingress region of a primary path (paragraph [0020])**, where the ingress region comprises a link associated with the source network device, and the link comprises either an outgoing link or a link between the source network device and a neighboring network device** (Figure 1; paragraphs [0004], [0016] through [0018])**;**

re-routes traffic from the primary path associated with an original Internet Protocol (IP) address to an alternate path which includes the device using a forwarding table that includes IP and Multi-Protocol Label Switched (MPLS) routing information (paragraph [0020])**while associating the original IP address to the alternate path upon detection of the failure** (paragraph [0020])**; and**

allows traffic to travel along the primary path when the failure is no longer detected along the ingress region (paragraph [0020])**.**

In order to make the overview set forth above concise the disclosure that has been included, or referred to, above only represents a portion of the total disclosure set forth in the Specification that supports the independent claims.

(ii). The Remainder of the Specification Also Supports the Claims

The Appellants note that there may be additional disclosure in the Specification that also supports the independent and dependent claims. Further, by including the specification citations in parenthesis above the Appellants do not represent that this is the only evidence that supports the independent claims nor do Appellants necessarily represent that these citations

alone can be used to fully interpret the claims of the present invention. Instead, the citations provide background support as an overview of the claimed subject matter.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL:

Appellants seek the Board's review and reversal of the rejection of: (a) claims 1, 3-5, 7-9, 11-13, 15-17, 19-21 and 23-29 under 35 U.S.C.§103(a) based on the combination of Kanakubo and Skalecki; (b) claims 1, 3-5, 7-9, 11-13, 15-17, 19-21 and 23-29 under 35 U.S.C.§103(a) based on the combination of Dantu and Skalecki; and (c) claims 1, 3-5, 7-9, 11-13, 15-17, 19-21 and 23-29 under 35 U.S.C.§103(a) based on a combination of Dantu and Anderson.

As a preliminary matter, the Appellants note that it is sometimes difficult to tell what reference the Examiner is relying upon as disclosing a particular claimed feature. Further, it is unclear whether some of the stated rejections, based on 35 U.S.C.§103(a), are really based on 35 U.S.C.§102. Appellants request clarification of the Examiner's rejections.

VII. ARGUMENTS:

A. The Section 103 Rejections Based on Kanakubo and Skalecki

Claims 1, 3-5, 7-9, 11-13, 15-17, 19-21 and 23-29 were rejected under 35 U.S.C.§103(a) based on the combination of Kanakubo and Skalecki. Appellants disagree for at least the following reasons.

(i) claims 1, 9 and 17

Of claims 1, 3, 4, 9, 11, 17, 19 and 20, claims 1, 9 and 17 are independent claims and it is to these claims that the Appellants direct their attention.

Each of independent claims 1, 9 and 17 include the features of: (a) detecting a failure along an ingress region of a primary path; and (b) re-routing

traffic from the primary path associated with an original Internet Protocol (IP) address to an alternate path...while associating the original IP address to the alternate path upon detection of the failure.

Turning first to Kanakubo and feature (a), Kanakubo repeatedly refers to "remote fault" detection (see, for example, paragraphs [0015]) and ([0034]).

Kanakubo also states that, "[i]n the case where a fault occurrence 'a1' of label switched path is detected in the label switching router (LSP-F) 3 other than the label switching router (LSP-P) 1" a "fault indication retrieval table" is retrieved (see paragraph [0027]). In other words, Kanakubo appears to be directed to faults other than those involving a source router (LSP-P is a source router).

Taken together, the most reasonable interpretation of these statements is that Kanakubo is not directed at the detection of a fault along the claimed ingress portion of a primary path as in claims 1, 9, and 17 (and their dependent claims). Instead, it is directed at the detection of faults that occur at locations that are remote from an ingress region or source router.

The Examiner's position appears to be that the 'ingress region' can be anywhere in the network as long as the region is input/incoming region/area/paths of the network. This is impermissible. Further, regardless of the Examiner's interpretation, the Examiner appears to ignore the teachings in Kanakubo that teach away from ingress region, fault detection.

As the Examiner knows well, though claims may be interpreted broadly any interpretation must be reasonable in light of the specification, *In re Hyatt*, 54 USPQ 2d 1664, 1667 (Fed.Cir. 2000). The specification provides two examples of an "ingress region". The first is "along an outgoing link associated with a source network device" (paragraph [0004]). The second is "at a network device which neighbors the source network device, a so-called neighboring device" (paragraph [0004]).

Thus, the Examiner's interpretation of the phrase "ingress region" is impermissible because it is not reasonable in light of the teachings of the specification.

Further, to the extent Kanakubo's disclosure can be understood, the fault shown in Fig.1 is not along an outgoing link associated with a source network device (e.g., LSR-P 1) or at a network device (e.g., LSR 2) which neighbors the source network device. This fact coupled with Kanakubo's apparent focus on remote fault detection leads to the conclusion that Kanakubo does not disclose the ingress region, fault detection features set forth in claims 1, 9, and 17 (and their dependent claims).

Turning to feature (b), instead of disclosing the claimed re-routing feature Kanakubo appears to suggest the opposite; namely, that the address of a primary path is replaced with a different address when an alternative path is used.

Fig. 3 of Kanakubo depicts a "LSP Fault Indication Retrieval Table" ("Table"). To the extent that the description of this Table can be understood, it does not appear that the Table includes a value that indicates an original IP address of a primary path is associated with an alternative path.

Paragraphs [0039] through [0045] describe the contents of Kanakubo's Table. More particularly: the column in the Table labeled "Indicated Protection Point" appears to identify the IP address of a router that will be used as a "protection point" (e.g., address of the first router in an alternative path, see paragraphs [0040] and [0042] through [0045]) or the address of a router that will "stop the [differentiated] service" (see paragraph [0041]); the column labeled "Entry Type" describes the type of path (see paragraphs [0040] and [0042] through [0045]); and the column labeled "Entry" identifies the routers that are to be bypassed (see paragraphs [0040] and [0042] through [0045]). There does not appear to be any entry in Kanakubo's Table that indicates that

an original IP address of a primary path becomes associated with an alternative path.

In fact, Kanakubo appears to be mostly silent as to the details of its address association (i.e., in Kanakubo terminology, how packets are switched from one path to another). For example, Kanakubo states that after a "fault indication packet is received.....the switching of the corresponding label switched path is performed (step S8 in Fig. 6)" (see paragraph [0053]). However, thereafter, no details of the switching process appear to be described.

Further, to the extent Kanakubo does discuss its switching process, it appears to imply that, switching from a primary path to a secondary path "may involve replacement of the label value" (see paragraph [0055]). Said another way, rather than use the original address of a primary path as the address of an alternative path the original address is replaced with a different address.

As for Skalecki, it too fails to disclose features (a) and (b). Skalecki explicitly discusses a fault that is located outside of an ingress region, between downstream nodes "H" and "K" (*see* paragraph [0043]). There is no mention of ingress region, fault detection in Skalecki.

Further, despite the Examiner's contentions, Skalecki is silent with respect to the re-routing of traffic from a primary path associated with an original Internet Protocol (IP) address to an alternate path....<u>while associating the original IP address to the alternate path upon detection of the failure</u>. Instead, it appears that Skalecki creates a separate protection path, "P1", having its own address, to route traffic away from original working path, "W1", without using the address of W1. There is no discussion within Skalecki which indicates that W1's address is associated with P1 upon detection of a fault between downstream nodes H and K.

(ii) claims 25 and 28

Of claims 25-29, claims 25 and 28 are independent claims and it is to these claims that the Appellants direct their attention.

Though similar to claims 1, 9 and 17, claims 25 and 28 include more details concerning the ingress region of a primary path. Claim 25 specifies that the ingress region of a primary path "comprises a link associated with [a] source network device" while claim 28 specifies that the ingress region comprises "a link associated with [a] source network device, and the link comprises either an outgoing link or a link between the source network device and a neighboring network device".

Even if Kanakubo and/or Skalecki can somehow be interpreted as disclosing the ingress regions of claims 1, 9 and 17 in no way can they be interpreted as disclosing the ingress regions of claims 25 and 28.

Instead, as set forth above, Kanakubo appears to be directed at the detection of faults that occur at locations that are remote from an ingress region or source router while Skalecki appears to disclose the detection of fault between downstream nodes.

Claims 25 and 28 (and their dependent claims) also include the feature of associating an original IP address to an alternate path upon detection of a failure. For the reasons set forth above with respect to claims 1, 9 and 17 neither Kanakubo nor Skalecki discloses or suggests this feature.

(iii) claims 5, 13 and 21

Of claims 5-7, 8, 13, 15, 16, 21, 23 and 24, claims 5, 13 and 21 are independent claims and it is to these claims that the Appellants direct their attention.

Each of independent claims 5, 13 and 21 include the feature of re-routing traffic from a primary path associated with an original IP address to an

alternate path while maintaining the original address. As discussed above with respect to claims 1, 9, 17, 25 and 28, neither Kanakubo nor Skalecki appears to disclose or suggest this feature.

B. The Section 103 Rejections Based On Dantu and Skalecki

Claims 1, 3-5, 7-9, 11-13, 15-17, 19-21 and 23-29 were rejected under 35 U.S.C.§103(a) based on the combination of Dantu and Skalecki. Appellants disagree.

(i) claims 1, 9 and 17

Of claims 1, 3, 4, 9, 11, 17, 19 and 20, claims 1, 9 and 17 are independent claims and it is to these claims that the Appellants direct their attention.

Each of independent claims 1, 9 and 17 include the features of: (a) detecting a failure along an ingress region of a primary path; and (b) re-routing traffic from the primary path associated with an original Internet Protocol (IP) address to an alternate path....while associating the original IP address to the alternate path upon detection of the failure.

Regarding feature (a), rather than disclose the detection of a failure along an ingress region of a primary path, Dantu appears to disclose the detection of a failure along a link between two non-ingress, network nodes 344, 348.

The Examiner appears to interpret Dantu's statement that each node within the fiber optic ring network shown in Figure 3 "may serve as an ingress node" (column 9, lines 9-10) as inferring that the failure between nodes 344 and 348 is along an ingress region. This is incorrect. While any one of the nodes in Figure 3 could be connected to the Internet shown in Figure 3, thereby becoming an ingress node, this would also change the role and functions of the remaining nodes as well as, thereby altering Dantu's discussion of its failure detection. The fact is that Dantu explicitly depicts a failure occurring outside an ingress region and explicitly selects node 300, not

nodes 344 or 348, as an ingress node to explain its technique (see column 9, lines 7-9).

Further, the claims are directed at failures along an ingress region of a primary path, not at the well known concept of an "ingress node" itself. So, the fact that Dantu discloses that its ingress node can be any one of a number of nodes connected to the Internet is irrelevant.

Regarding feature (b), Dantu's discussion of fault detection and the use of protection paths occurs mainly in column 9, line 42 to column 12, line 38 and column 17, line 12 to column 20, line 30. Nowhere in this discussion does it appear that Dantu states, explicitly or implicitly, that the original address of a primary path becomes associated with (or is "maintained") by, an alternative path. To the contrary, Dantu appears to imply that addresses are changed. For example, Dantu states that: "After the identifying step 1004, the ingress node 300 determines appropriate protection path label values for the affected data packets and sets the labels into the header of the outgoing data packets (step 1008). Finally, the affected data packets are generated onto the fiber optic ring network and are forwarded along the protection paths according to the newly set label values".

Nor does Skalecki make up for the deficiencies in Dantu, as explained above with respect to independent claims 1, 9 and 17.

(ii) claims 5, 13 and 21

Of claims 5-7, 8, 13, 15, 16, 21, 23 and 24, claims 5, 13 and 21 are independent claims and it is to these claims that the Appellants direct their attention.

Independent claims 5, 13 and 21 include the features of (a) re-routing traffic from a primary path associated with an original IP address to an alternate path while maintaining the original address, (b) where the alternate path comprises devices which are not a part of the primary path except for a

network device that has received a failure message and a destination network device.

Turning first to Dantu and feature (a), Dantu does not disclose or suggest such a feature as discussed above with respect to claims 1, 9 and 17.

Nor does Dantu disclose or suggest feature (b). Instead, in Dantu, upon detection of a "link failure" packets are transmitted through a "protection path" which includes nodes that are also a part of an original "working path", where the nodes are other than the network device that has received a failure message and destination network device.

Nor does Skalecki make up for the deficiencies in Dantu. More specifically, the Examiner does not appear to take the position that Skalecki discloses or suggests feature (b). As for feature (a), Skalecki does not disclose or suggest this feature as explained above with respect to claims 1, 9 and 17.

(iii) claims 25 through 29

Of claims 25-29, claims 25 and 28 are independent claims and it is to these claims that the Appellants direct their attention.

As discussed above, claim 25 specifies that the ingress region of a primary path "comprises a link associated with [a] source network device" while claim 28 specifies that the ingress region comprises "a link associated with [a] source network device, and the link comprises either an outgoing link or a link between the source network device and a neighboring network device".

Even if Dantu and/or Skalecki can somehow be interpreted as disclosing the ingress regions of claims 1, 9 and 17 in no way can they be interpreted as disclosing the ingress regions of claims 25 and 28.

Instead, as set forth above, rather than disclose the detection of a failure along an ingress region of a primary path, Dantu appears to disclose the detection of a failure along a link between two non-ingress, network nodes

while Skalecki appears to disclose the detection of fault between downstream nodes.

Claims 25 and 28 also include the feature of associating an original IP address to an alternate path upon detection of a failure. For the reasons set forth above with respect to claims 1, 9 and 17 neither Dantu nor Skalecki discloses or suggests this feature.

C. The Section 103 Rejections Based on Dantu and Anderson

Claims 1, 3-5, 7-9, 11-13, 15-17, 19-21 and 23-29 were rejected under 35 U.S.C.§103(a) based on the combination of Dantu and Anderson. Appellants disagree for at least the following reasons.

(i) claims 1, 5, 9, 13, 17, 21, 25 and 28

Of claims 1, 3-5, 7-9, 11-13, 15-17, 19-21 and 23-29, claims 1, 5, 9, 13, 17, 21, 25 and 28 are independent and it is to these claims that the Appellants direct their attention

Each of the claims includes the feature of re-routing traffic from a primary path associated with an original IP address to an alternate path using a forwarding table that includes IP and MPLS routing information. Though it is difficult for the Appellants to determine which of the two references the Examiner is relying upon for the disclosure of this feature, nonetheless, the Appellants submit that any combination of Dantu and Anderson is impermissible because such a combination requires one or both of the references to change their principle of operation.

For example, as far as the Appellants can tell Anderson is directed at Virtual Path and Virtual Connection based protection switching while Dantu is directed at MPLS, IP protocol based protection switching. The Examiner's suggested combination would require Anderson to change its principle of operation from VP/VC based protection switching to IP based protection switching. Accordingly, because the Examiner's suggested combination would

require Anderson to change its principle of operation such a combination is impermissible. Nor would one skilled in the art equate VP/VC protection switching methods and devices with the claimed MPLS, IP protocol failure detection methods or devices.

(ii) claims 1, 9, 17, 25 and 28

Of claims 1, 3, 4, 9, 11, 12, 17, 19, 20, and 25-29, claims 1, 9, 17, 25 and 28 are independent claims and it is to these claims that the Appellants direct their attention.

Each of claims 1, 9, 17, 25 and 28 include the feature of detecting a failure along an ingress region of a primary path. As discussed above in section B., Dantu does not disclose this feature. Anderson does not make up for this deficiency in Dantu.

"Primary" paths are used in MPLS-based networks, not VP/VC based networks. Because Anderson is directed at the latter and not the former, there is no discussion whatsoever of primary paths within Anderson, much less a discussion of the detection of a failure along the ingress region of a primary path.

In addition each of these claims includes the feature of associating an original IP address of a primary path to an alternate path upon detection of a failure or the maintenance of such an address by the alternative path. As discussed above in section B, Dantu does not disclose or suggest such a feature. Nor does Anderson make up for this deficiency. There is no discussion whatsoever within Anderson of the association of a primary path, IP address to an alternate path upon detection of a failure or the maintenance of such an address by the alternative path.

Further, because Anderson is directed at VP/VC based routing, which uses a different routing scheme than MPLS, IP based routing, one skilled in the art would not equate Anderson' VP/VC protection switching scheme with the claimed MPLS, IP based failure detection methods or devices.

(iii) claims 5, 13 and 21

Of claims 5-7, 8, 13, 15, 16, 21, 23 and 24, claims 5, 13 and 21 are independent claims and it is to these claims that the Appellants direct their attention.

Each of claims 5, 13 and 21 includes the feature of re-routing traffic from a primary path associated with an original IP address to an alternate path using a forwarding table that includes IP and MPLS routing information, said rerouting maintaining the original address. As discussed above in sction B, Dantu does not disclose such re-routing. Anderson does not make up for this deficiency in Dantu.

"Primary" paths are used in MPLS-based networks, not VP/VC based networks. Because Anderson is directed at the latter and not the former, there is no discussion whatsoever of primary paths within Anderson, much less a discussion of the re-routing of primary paths.

In addition each of these claims includes the feature of maintaining the original address of the primary path as the address of the alternate path after the traffic has been re-routed to the alternate path. As discussed above in section B, Dantu does not disclose or suggest such a feature. Nor does Anderson make up for this deficiency as just discussed above with respect to claims 1, 9, 17, 25 and 28.

Conclusion:

Appellants respectfully request that members of the Board reverse the decision of the Examiner and allow claims 1, 3-5, 7-9, 11-13, 15-17, 19-21 and 23-29.

The Commissioner is authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 50-3777 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17; particularly, extension of time fees.

Respectfully submitted,

Capitol Patent & Trademark Law Firm, PLLC

By: /John E. Curtin/

John E. Curtin, Reg. No. 37,602

P.O. Box 1995
Vienna, VA 22183
(703)266-3330

VIII. CLAIMS APPENDIX

1. A network device, wherein the device:

detects a failure along an ingress region of a primary path;

re-routes traffic from the primary path associated with an original Internet Protocol (IP) address to an alternate path which includes the device using a forwarding table that includes IP and Multi-Protocol Label Switched (MPLS) routing information while associating the original IP address to the alternate path upon detection of the failure; and

allows traffic to travel along the primary path when the failure is no longer detected along the ingress region.

2. (Canceled).

3. The device of claim 1 wherein, the device is a multi-protocol label switched (MPLS) device and the primary and alternate paths are label switched paths (LSPs).

4. The device of claim 1 wherein the failure is at a neighboring network device or along a link between the device and the neighboring network device.

5. A network device, wherein the device:

receives a failure message;

re-routes traffic from a primary path associated with an original IP address to an alternate path using a forwarding table that includes IP and MPLS routing information, said rerouting maintaining the original address, the alternate path comprising devices which maintain a same quality of service as

the primary path and are not a part of the primary path except for the network device and a destination network device; and

allows traffic to travel along the primary path when the failure is no longer detected.

6. (Canceled).

7. The device of claim 5 wherein, the network device is a MPLS device and the primary and alternate paths are LSPs.

8. The device of claim 5 wherein, the quality of service is associated with at least one of the set consisting of bandwidth, delay, delay jitter, and packet loss rate.

9. A method for re-routing traffic comprising the steps of:

detecting a failure along an ingress region of a primary path;

re-routing traffic from the primary path associated with an original IP address to an alternate path which includes a source device using a forwarding table that includes IP and MPLS routing information while associating the original address to the alternate path upon detection of the failure; and

allowing traffic to travel along the primary path when the failure is no longer detected along the ingress region.

10. (Canceled).

11. The method of claim 9 wherein the primary and alternate paths are LSPs.

12. The method as in claim 9 wherein the failure is at a neighboring network device or along a link between the initiating device and the neighboring network device.

13. A method for re-routing traffic comprising the steps of:

receiving a failure message;

after said receiving step, re-routing traffic from a primary path associated with an original IP address to an alternate path using a forwarding table that include IP and MPLS routing information, said rerouting maintaining the original address, the alternate path comprising devices which maintain a same quality of service as the primary path and are not a part of the primary path except for an initiating network device and a destination network device; and

allowing traffic to travel along the primary path when the failure is no longer detected.

14. (Canceled).

15. The method of claim 13 wherein the primary and alternate paths are LSPs.

16. The method of claim 13 wherein, the quality of service is associated with at least one of the set consisting of bandwidth, delay, delay jitter, and packet loss rate.

17. A network device comprising:

means for detecting a failure along an ingress region of a primary path;

means for re-routing traffic from the primary path associated with an original IP address to an alternate path which includes the device using a forwarding table that includes Internet Protocol (IP) and Multi-Protocol Label Switched (MPLS) routing information while associating the original IP address to the alternate path upon detection of the failure; and

means for allowing traffic to travel along the primary path when the failure is no longer detected along the ingress region.

18. (Canceled).

19. The device of claim 17 wherein the device is a MPLS device and the primary and alternate paths are LSPs.

20. The device of claim 17 wherein the failure is at a neighboring network device or along a link between the device and the neighboring network device.

21. A network device comprising:

means for receiving a failure message;

means for re-routing traffic from a primary path associated with an original IP address to an alternate path using a forwarding table that includes IP and MPLS routing information, said means for re-routing maintaining the original address, the alternate path comprising devices which maintain a same quality of service as the primary path and are not a part of the primary path except for the network device and a destination network device; and

means for allowing traffic to travel along the primary path when the failure is no longer detected.

22. (Canceled).

23. The device of claim 21 wherein, the network device is a MPLS device and the primary and alternate paths are LSPs.

24. The device of claim 21 wherein, the quality of service is associated with at least one of the set consisting of bandwidth, delay, delay jitter, and packet loss rate.

25. A source network device, wherein the device:

detects a failure along an ingress region of a primary path, where the ingress region comprises a link associated with the source network device;

re-routes traffic from the primary path associated with an original Internet Protocol (IP) address to an alternate path which includes the device using a forwarding table that includes IP and Multi-Protocol Label Switched (MPLS) routing information while associating the original IP address to the alternate path upon detection of the failure; and

allows traffic to travel along the primary path when the failure is no longer detected along the ingress region.

26. The device of claim 25 wherein, the device is a multi-protocol label switched (MPLS) device and the primary and alternate paths are label switched paths (LSPs).

27. The device of claim 25 wherein the link associated with the source network device is an outgoing link or a link between the source network device and a neighboring network device.

28. A source network device, wherein the device:

detects a failure along an ingress region of a primary path, where the ingress region comprises a link associated with the source network device, and the link comprises either an outgoing link or a link between the source network device and a neighboring network device;

re-routes traffic from the primary path associated with an original Internet Protocol (IP) address to an alternate path which includes the device using a forwarding table that includes IP and Multi-Protocol Label Switched (MPLS) routing information while associating the original IP address to the alternate path upon detection of the failure; and

allows traffic to travel along the primary path when the failure is no longer detected along the ingress region.

29. The device of claim 28 wherein, the device is a multi-protocol label switched (MPLS) device and the primary and alternate paths are label switched paths (LSPs).

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.